(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－265867

(43)公開日　平成５年(1993)10月15日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/14	３２０　Ｃ	9293－5B		
15/78	５１０　Ｋ	7530－5Ｌ		

審査請求　未請求　請求項の数２(全　７　頁)

(21)出願番号　特願平4－64424

(22)出願日　平成４年(1992)３月23日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　岡本　渉
東京都港区芝五丁目７番１号日本電気株式会社内

(74)代理人　弁理士　京本　直樹　(外２名)

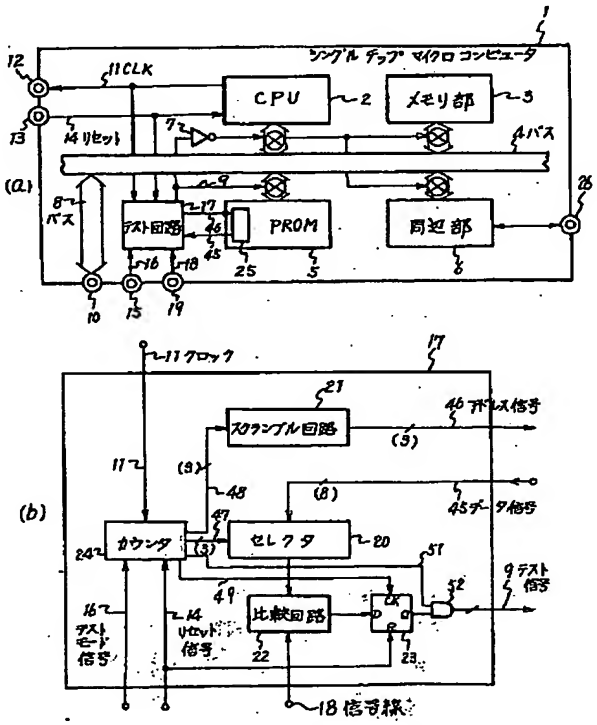
(54)【発明の名称】　シングルチップマイクロコンピュータ

(57)【要約】

【目的】外部からパスワードを入力することによりテストモードを許可し、内蔵ＰＲＯＭ格納データを保護する。

【構成】テストモードを許可する回路を、スクランブル回路２１，比較回路２２，カウンタ２４，セレクタ２０で構成し、外部よりシリアルに信号１８によりパスワードを入力すると共に、スクランブル回路２１の出力をアドレスとして内蔵ＰＲＯＭ５からデータをリードしセレクタ２０を介して１ビット単位にて比較する。また、カウンタ２４にて比較回数を計数し、一定回数に達すると比較を停止させる。比較回路２２はＰＲＯＭの格納データと外部からの入力パスワードを比較し、一致する場合のみ信号９を出力してテストモードを許可する。

【効果】内蔵ＰＲＯＭに格納した秘匿性の高いデータへのアクセスが困難となり、悪用される危険も小さくなる。



1

【特許請求の範囲】

【請求項１】　単一半導体基板上に中央処理装置，記憶部，周辺部およびプログラマブルＲＯＭ（以下ＰＲＯＭという）を集積し、このＰＲＯＭに対しテスト機能を内蔵したシングルチップマイクロコンピュータにおいて、テスト時にクロックを計数するカウンタと、このカウンタの出力アドレスを入替え反転しアドレス信号として出力するスクランブル回路と、前記アドレス信号に対応した前記ＰＲＯＭのデータを前記カウンタの出力により選択するセレクタと、このセレクタの出力と外部から入力したデータ値を比較する比較回路とから構成されるテスト回路を付加し、外部から入力した値と前記ＰＲＯＭの格納値とが等しい場合のみ外部から前記ＰＲＯＭへのアクセスを可能とするようにしたことを特徴とするシングルチップマイクロコンピュータ。

【請求項２】　テスト回路が、ＰＲＯＭの格納値に対するアドレス指定を、このＰＲＯＭに格納したデータにより行なうものである請求項１記載のシングルチップマイクロコンピュータ。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、単一半導体基板上にメモリ機能及びコンピュータ機能を集積したシングルチップマイクロコンピュータに関し、特に内蔵ＰＲＯＭに格納した値に対応したデータを外部から入力した場合のみテスト可能としたシングルチップマイクロコンピュータに関する。

【０００２】

【従来の技術】近年、ＬＳＩ製造技術の進歩によりシングルチップマイクロコンピュータ（以下シングルチップマイコンという）の分野においても高集積化が進み、単位機能当たりのコストの低下も著しくなってきている。

【０００３】従来、銀行などの金融機関においては磁気カードが主に使用されてきたが、磁気カードは記憶容量が少なく、またセキュリティの面で問題があり、最近では不正使用、偽造など多くの犯罪が頻発し、大きな社会問題となっている。そこでこの磁気カードに代るものとして、シングルチップマイコンを搭載したＩＣカードが登場し、国内外において実用化に向けて大規模な実験が進んでいる。このＩＣカードは磁気カードに比べて記憶容量も数段大きく、またカード内にコンピュータ機能を内蔵しているのでセキュリティの面でも格段の信頼度がある。

【０００４】一般にシングルチップマイコンを搭載したＩＣカードにおいては、データメモリの大部分にＵＶＥＰＲＯＭ（Ｕｌｔｒａ－Ｖｉｏｌｅｔ　ＥｒａｓａｂｌｅＰｒｏｇｒａｍｍａｂｌｅ　ＲＯＭ）またはＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　ＲＯＭ）を使用しており（以下ＵＶＥＰＲＯＭ、ＥＥＰＲＯＭをＰＲＯＭという）、そ

2

のデータメモリをいくつかの領域に分割しそのアクセスを管理している。

【０００５】銀行などの金融機関の発行するキャッシュカード、クレジットカードとしてＩＣカードを使用する場合、この分割されたデータメモリの一部をシークレット・ゾーン（Ｓｅｃｒｅｔ　Ｚｏｎｅ）と呼び、銀行の口座番号，ＩＤナンバー，シークレットナンバーなど機密性の高いデータを格納するのに使用している。このシークレット・ゾーンはＩＣカードの不正使用、偽造を防止する上で重要な部分であって、使用時にはソフトウエアによりその領域に対するアクセスを管理し、特別な場合だけ前記領域に対しアクセスできるようになっている。ところが、テストモード時には、容易に外部より内蔵ＰＲＯＭの全領域に直接アクセスが可能であり、シークレット・ゾーン内の値を読み出して悪用したり、故意に変更することが可能であった。

【０００６】図６はこの種のシングルチップマイコンの一例のブロック図である。図６において、メモリ部３はユーザプログラム格納及びデータの格納に用いる読出し専用または、読出し書込ともに可能なメモリ、内部バス４はアドレス及びデータを時分割に転送するバス、内部バス８は、テストモード時に、外部端子１０を介して内部バス４にアドレス及びデータを転送する際に用いる時分割バスである。

【０００７】中央処理装置（以下ＣＰＵという）２は、メモリ部３に格納したプログラムに従って、データ処理を行なう。周辺部６は、チップ外部との通信を行なうためのポート等から構成され、内部バス４を介して入力したデータを外部端子２６に出力し、外部端子２６からデータを入力し、内部バス４に出力する機能を持つ。ＰＲＯＭ５は、データメモリとしてＵＶＥＰＲＯＭまたはＥＥＰＲＯＭから構成され、メモリ内にシークレット・ゾーン２５を設け、カードのＩＤナンバー，シークレットナンバー，口座番号等を格納しており、ＣＰＵの命令により読出し及び書込みを行なう。このシークレット・ゾーン２５へのアクセス管理は、ユーザがソフトウエアにより行なっている。。

【０００８】端子１５は、テストモード時に「１」とする外部入力端子であり、この時インバータ７の出力が０となるため内部バス４にはＰＲＯＭ５のみ接続され、ＰＲＯＭ５へのアクセスがチップ外部より直接可能となる。端子１０は、内部バス８を介してアドレス及びデータを外部に入出力する端子であり、内部バス４に接続され、端子１２はＣＰＵ２の出力するＣＰＵクロック１１を出力する端子、端子１３はＣＰＵ２をリセットする端子で、「１」の時リセット信号１４が「１」となりＣＰＵ２をリセットする。

【０００９】次にテスト時の動作を説明する。端子１３を「１」のまま端子１５を「１」とし、端子１３をＣＰＵクロック１１の立下りに同期して０とする。この時、

テスト信号９は「１」となりインバータ７の出力は「０」となるのでＣＰＵ２、メモリ部３、周辺部６は内部バス４から電気的に切離される。従って、内部バス４に接続されているのはＰＲＯＭ５のみとなる。この状態で外部端子１０、内部バス８を介してアドレス及びデータをＰＲＯＭ５に入力し、データの読出し及び書込みを行なう。この時、シークレットゾーン２５のアドレスを入力すれば容易にゾーン内データにアクセス可能である。従って、データリード及びライトが容易に行なえることとなる。

【００１０】以上述べたように従来のシングルチップマイコンにおいては、秘匿データを格納するシークレット・ゾーンに対するアクセス管理をすべてユーザーのソフトウエアにより行なっている。このようなシングルチップマイコンをカードに搭載した場合、テストモードを使用することにより、シークレット・ゾーンに対し不当なデータアクセスを行なうことが可能である。さらにデータメモリに電気消去型読み出し専用メモリ（ＥＥＰＲＯＭ）が使用されている場合には、書込み命令が実行されるとＰＲＯＭ内部で自動的に書込み用の電圧が生成されるので、シークレット・ゾーンに対し、不当な書込みが容易に行なうことが可能である。

【００１１】

【発明が解決しようとする課題】上述したように従来のデータメモリにおいて、アクセス保護の領域であるシークレット・ゾーンへのアクセスを管理しているシングルチップマイコンにおいては、内蔵ＰＲＯＭへのアクセス管理をすべてソフトウエアによって行なっているので、テストモード時に容易にアクセス可能であり、不正なアクセスが行われてシークレット・ゾーン内のデータが悪用されたり、また故意にデータが書き換えられる危険性が在るという欠点が存在した。

【００１２】本発明の目的は、簡単なテスト回路を付加することにより、テストモード時の不当なアクセスを排除し、より確実なセキュリテイが容易に得られるようにしたシングルチップマイコンを提供することにある。

【００１３】

【課題を解決するための手段】本発明の構成は、単一半導体基板上に中央処理装置，記憶部，周辺部およびプログラマブルＲＯＭ（以下ＰＲＯＭという）を集積し、このＰＲＯＭに対しテスト機能を内蔵したシングルチップマイクロコンピュータにおいて、テスト時にクロックを計数するカウンタと、このカウンタの出力アドレスを入替え反転しアドレス信号として出力するスクランブル回路と、前記アドレス信号に対応した前記ＰＲＯＭのデータを前記カウンタの出力により選択するセレクタと、このセレクタの出力と外部から入力したデータ値を比較する比較回路とから構成されるテスト回路を付加し、外部から入力した値と前記ＰＲＯＭの格納値とが等しい場合のみ外部から前記ＰＲＯＭへのアクセスを可能とするようにしたことを特徴とする。

【００１４】

【実施例】図１（ａ），（ｂ）は本発明の第１の実施例のシングルチップマイコンのブロック図およびそのテスト回路１７のブロック図である。本実施例においては、新たに追加したテスト回路１７以外の構成要素は、図６の従来例と相違がない。従ってテスト回路１７を中心に説明する。

【００１５】図において、テスト回路１７は、ＣＰＵの出力するクロック信号１１に同期して外部端子１９よりシリアルにデータを入力し、ＰＲＯＭ５内のシークレットゾーン２５に格納した値と外部より入力した、ビットシリアルデータ値を比較して、一致する場合のみテストモードを許可する機能を有する。

【００１６】本実施例のテスト回路１７は、図１（ｂ）のように、ラッチ回路２３，スクランブル回路２１，比較回路２２，カウンタ２４，２入力ＡＮＤゲート５２から構成される。スクランブル回路２１は、カウンタ２４の出力するＰＲＯＭアドレス４８をスクランブルし、ＰＲＯＭ５に対しアドレス信号４６を出力する。セレクタ２０は、カウンタ２４の出力するセレクト信号４７に従って、入力データから１ビットをセレクトし比較回路２２に対して出力する。比較回路２２は、セレクタ２０の出力と、外部からの入力データ１８を比較し、一致した時に「１」を、一致しない時は「０」をラッチ回路２３に対して出力する。

【００１７】カウンタ２４は、リセット信号１４の立下りに同期してカウントデータをロードし、基本クロック１１の立上りに同期し、テストモード信号１６が「１」で、リセット信号１４が「０」の時のみ、ＣＰＵクロック１１をダウンカウントする。ラッチ回路２３は、カウンタ２４の出力するカウント信号４９の立下り同期で比較回路２２の出力をラッチし、ＡＮＤゲート５２に対して出力する。また、リセット信号１４が「１」の時「０」にクリアされる。ラッチ回路２３は、リセット信号１４が「０」の時「１」をラッチ後「０」をラッチすると、以後リセット信号１４が再度「１」になるまで「０」を保持する。ＡＮＤゲート５２は、ラッチ回路２３の出力とカウンタ２４の出力する制御信号５１を入力とし、ＡＮＤ出力をテスト信号９として出力する。

【００１８】以下、テスト回路１７の動作を図２のタイミング図を用いて説明する。まず、リセット信号１４を「１」のままテストモード信号１６を「０」としておく。次に、テスト信号モード１６を「１」とし、リセット信号１４をＣＰＵクロック１１の立下りに同期して「０」とする。この時、リセット信号１４の立下りでラッチ回路２３はクリアされる。またカウンタ２４は、内蔵のダウンカウンタ及びラッチに初期値をロードする。以下、ダウンカウンタへのロードを「７」，ラッチへのロード値を「３」として説明する。

【００１９】ＣＰＵクロック１１の立上りに同期して外部端子１９よりシリアルに８ビットデータを入力する。この時、カウンタ２４は、ＣＰＵクロック１１の立上りに同期して８回カウントする。さらに、カウンタ２４のダウンカウンタへの格納値及びラッチの格納値を、各々３ビットのセレクト信号４７及び３ビットのＰＲＯＭアドレスとして出力する。スクランブル回路２１は、３ビットのＰＲＯＭアドレス４８をスクランブル（アドレス信号の入替え反転等）し、３ビットのアドレス信号４６としてＰＲＯＭ５に対し出力する。カウンタ２４内のダウンカウンタは、８回カウント動作後、制御信号５１を「１」にして停止する。

【００２０】比較回路２２は、セレクタ２０の出力する値と外部から入力する信号１８の値が同一の場合「１」をラッチ回路２３に対し出力する。また、同一でない場合「０」を出力する。セレクタ２０は、アドレス信号４６にてアドレスしたＰＲＯＭ５の格納データであるデータ信号４５に対し、カウンタ２４の出力するセレクト信号４７で指定する１ビットを選択して出力する。

【００２１】従って、本実施例のテスト回路１７においては、カウンタ２４がダウンカウントしながら出力するセレクト信号４７にて選択したＰＲＯＭ５内のデータであるデータ信号４５の１ビットと外部からの入力データである信号１８を、ビット単位に比較し結果をラッチ回路２３にラッチする。そしてダウンカウンタへのロード値にて指定されるビット数（ここでは８）だけ比較し、全ビットが一致した場合のみラッチ回路２３の最終値は「１」となる。また、カウンタ２４はダウンカウントを終了すると制御信号５１に「１」を出力するため、ＡＮＤゲート５２はテスト信号９に「１」を出力し、テストモードを許可する。

【００２２】この比較が、たとえ１ビットでも一致しない場合は、ラッチ回路２３の最終値は０となり、テスト信号９が「０」だからテストモードは禁止される。従って、カウンタ２４内のダウンカウンタへのロード値＋１で指定されるビットのパスワードを外部から入力し、ＰＲＯＭ５に内蔵したデータと一致した場合のみテストモードが許可されるため、従来に比べ不正にテストモードを実現することが困難である。さらに、パスワードのビットサイズも可変であり、かつＰＲＯＭ内のパスワード格納値に対するアドレスもスクランブルしてあるので、テストモードによる内蔵ＰＲＯＭへの不正なアクセスはますます困難となる。

【００２３】図３は図１のカウンタ２４の構成を示すブロック図である。このカウンタ２４は、定数発生回路４３，４ビットのダウンカウンタ４１，ＡＮＤゲート４４，３ビットラッチ４２から構成される。リセット信号１４が「１」の時、ダウンカウンタ４１はクリアされて、動作を停止し、ラッチ４２もクリアされる。リセット信号１４が「０」になると、立下り同期にて定数発生

回路４３の出力をラッチ４２及びダウンカウンタ４１の下位３ビットにロードする。また、テストモード信号１６が「１」のためダウンカウンタ４１はＡＮＤゲート４４の出力の立上りに同期してカウントダウンし、かつラッチ４２の格納値をＰＲＯＭアドレス４７として出力する。また、ダウンカウンタ４１はダウンカウントしながらカウンタの下位３ビットの内容をセレクト信号４８として出力し、カウンタの動作クロックをカウント信号４９として出力する。

【００２４】以下、ダウンカウンタ４１へのロード値を７として説明する。ダウンカウンタ４１は、８回ダウンカウントすると第１～第４ビットが「１」となるため、ＡＮＤゲート４４の出力も「０」となり、ダウンカウンタ４１はカウント動作を停止する。この時、セレクト信号４８は７～０まで８パタン出力される。従って、データ信号４５の全てのビットに対応してセレクト信号４８が出力される。

【００２５】本実施例においては、簡単なハードウエアから構成されるテスト回路１７を付加することにより、第三者によるテストモードの実現が容易でなくなり、シークレット・ゾーン２５内のデータに対する不当なアクセスやデータの消失を防ぐことができ、高度なフェール・セーフが実現される。

【００２６】図４及び図５は本発明における第２の実施例のシングルチップマイクロコンピュータのテスト回路のブロック図及び図４のカウンタのブロック図である。図４のブロック図は図１に対しＰＲＯＭ５からカウンタ２４ａへのパスが設けられている点でのみ相違している。従って、カウンタ２４ａの構成及び動作についてのみ述べる。

【００２７】本実施例のシングルチップマイコンのカウンタ２４ａは、図１のカウンタ２４に対して、ダウンカウンタ４１及びラッチ４２においてＰＲＯＭ５に内蔵した値を初期ロード値として指定する点で相違する。

【００２８】このカウンタ２４ａは、アドレス「０」のスクランブル値に対応してＰＲＯＭ２５より初期値をラッチ４２，ダウンカウンタ４１にロード後、ダウンカウント動作を行なう。すなわち、第１の実施例と異なり、定数発生回路４３の発生するロード値に代って、リセット信号１４をハイからロウに変化した時、クリアされたラッチ４２の格納値「０」をスクランブル回路２１にてスクランブル後アドレス信号４６にてアドレス指定し、ＰＲＯＭ５からリードしたデータ信号４５をロード値として、リセット信号１４の立下りにてラッチ４２にラッチする。従って・アドレス「０」をスクランブルしたアドレスに格納した値を変更することにより、パスワードの格納アドレスを変更可能であるため、第１の実施例に対しよりセキュリテイが高くなる効果がある。

【００２９】テスト回路１７ａは、ラッチ４２で指定したＰＲＯＭ５の格納データと外部からの入力データが一

致した場合のみテスト信号９を出力し、テストモードを実現する。初期値をラッチ４２、ダウンカウンタ４１にロードして以後の動作は第１の実施例と同様である。

【００３０】

【発明の効果】以上説明したように本発明においては、内蔵ＰＲＯＭに格納したデータと外部より入力したデータが一致する場合のみテストモードを許可するテスト回路を付加することにより、従来シークレット・ゾーンへのデータアクセスをテストモードの実現にて自由に行なっていた時に生じる不当なデータアクセスを禁止し、高度なセキュリティを実現する効果がある。

【図面の簡単な説明】

【図１】（ａ），（ｂ）は本発明の第１の実施例におけるシングルチップマイクロコンピュータおよびそのテスト回路のブロック図。

【図２】図１のテスト回路の動作を説明するタイミング図。

【図３】図１の実施例のテスト回路内カウンタのブロック図。

【図４】本発明の第２の実施例におけるテスト回路のブロック図。

【図５】図４のテスト回路内のカウンタのブロック図。

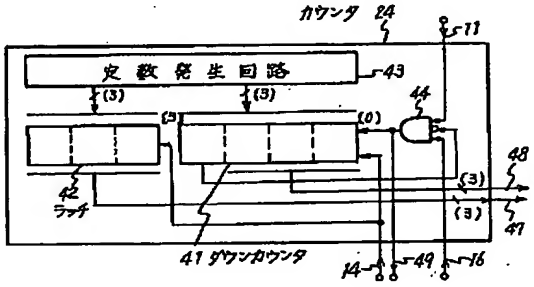
【図６】従来のシングルチップマイクロコンピュータの一例のブロック図。

【符号の説明】

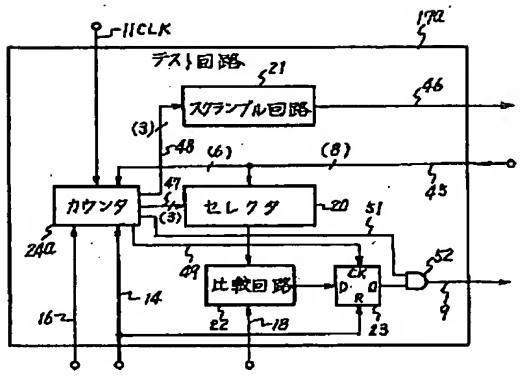
１，１ａ　シングルチップマイクロコンピュータ
２　ＣＰＵ
３　メモリ部

４，８　内部バス
５　ＰＲＯＭ
６　周辺部
７　インバータ
９　テスト信号
１０，～１３，１５，１９，２６　外部端子
１１　ＣＰＵクロック
１４　リセット信号
１６　テストモード信号
１７，１７ａ　テスト回路
１８　信号線
２０　セレクタ
２１　スクランブル回路
２２　比較回路
２３　ラッチ回路
２４，２４ａ　カウンタ
２５　シークレットゾーン
４１　ダウンカウンタ
４２　ラッチ
４３　定数発生回路
４４，５２　ＡＮＤゲート
４５　データ信号
４６　アドレス信号
４７　セレクト信号
４８　ＰＲＯＭアドレス
４９　カウント信号
５１　制御信号

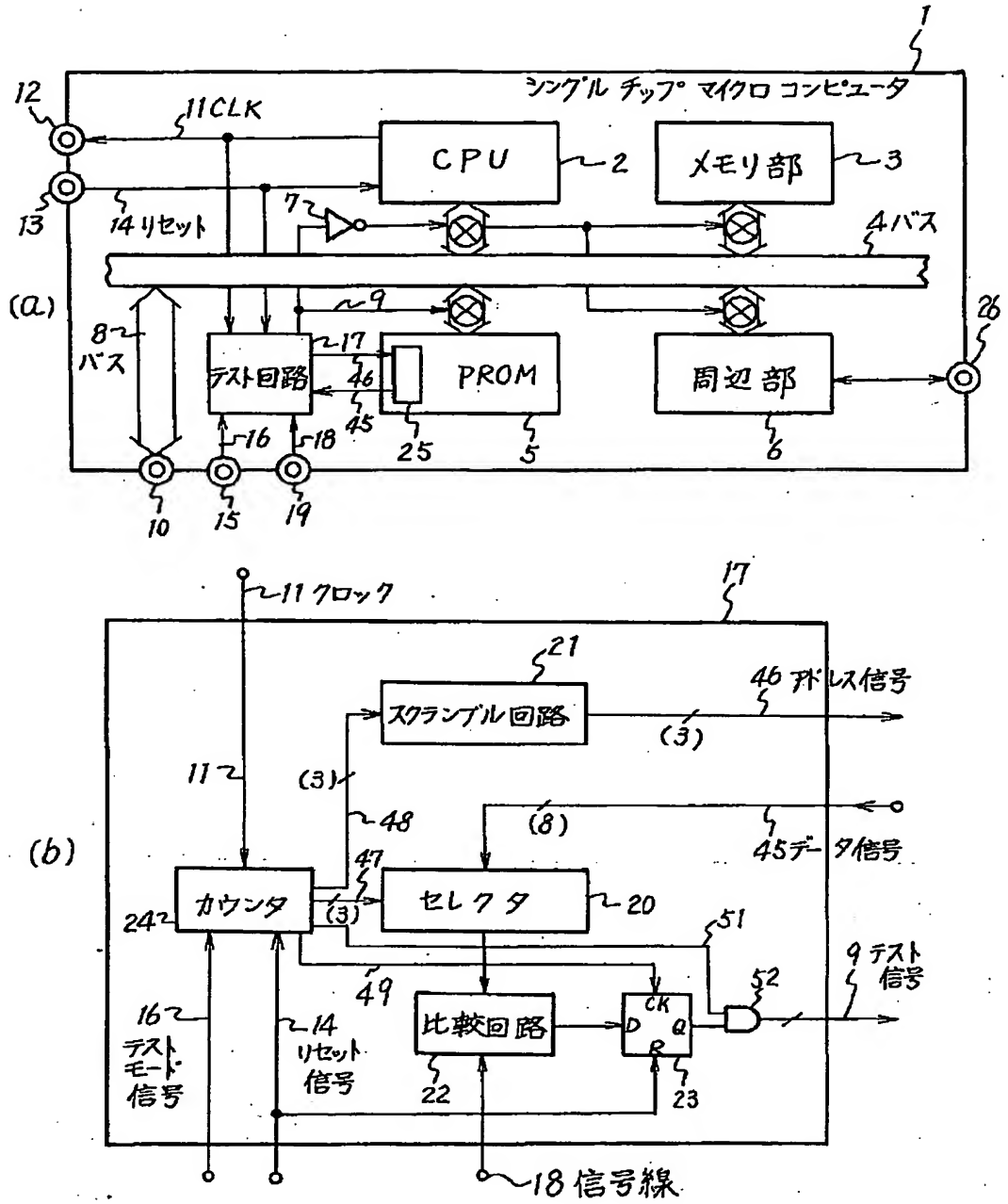
【図３】



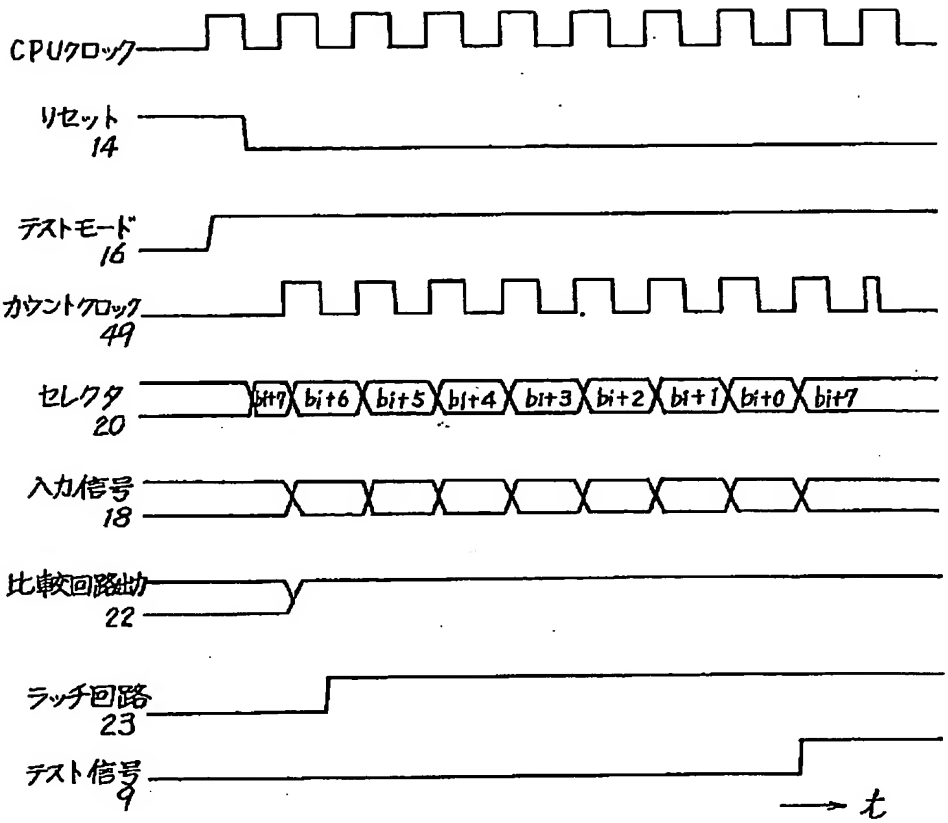
【図４】



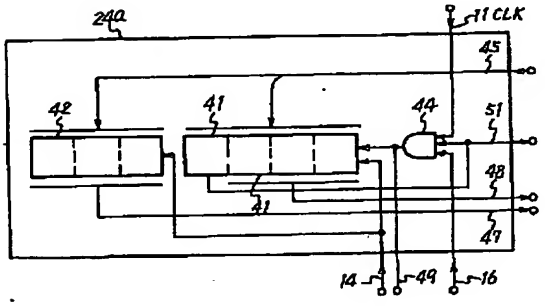
【図1】


1
シングル チップ マイクロ コンピュータ
12
11CLK
CPU
2
メモリ部
3
13
14リセット
7
4バス
(a)
8
バス
9
テスト回路
17
46
45
PROM
25
5
周辺部
6
26
16
18
10
15
19
11クロック
17
21
スクランブル回路
46アドレス信号
(3)
11
(3)
48
(8)
45データ信号
(b)
47
カウンタ
24
(3)
セレクタ
20
51
9テスト信号
52
49
16
テストモード信号
14
リセット信号
比較回路
CK
D
Q
R
22
23
18信号線

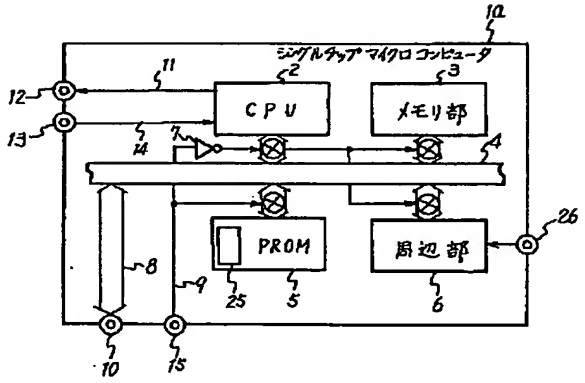
【図２】


CPUクロック
リセット
14
テストモード
16
カウントクロック
49
セレクタ
20
bit7
bit6
bit5
bit4
bit3
bit2
bit1
bit0
bit7
入力信号
18
比較回路出力
22
ラッチ回路
23
テスト信号
9
t

【図５】


24a
11 CLK
45
42
41
44
51
43
48
47
14
49
16

【図６】


10
シングルチップ マイクロコンピュータ
11
2
3
12
13
CPU
メモリ部
14
7
4
PROM
周辺部
26
8
9
25
5
6
10
15